GESSAR-II Appendix 15D.3, BWR/6
Probabilistic Risk Assessment (790 pages)

1.4.6 Reliability Model Definitions (Continued)

BOP systems are considered. Once core damage and fission product release is predicted in an accident sequence, no coolant injection system repair or recovery is considered. If adequate RPV water level has been maintained following accident initiation, on-line repair or recovery of containment heat removal, water injection, and diesel/generator (D/G) systems are modeled for components outside the primary containment for times prior to loss of containment integrity.

1.4.7 Initial and End-Point Conditions

Following the RSS approach, the reactor is assumed to have been at 100% power prior to accident initiation. Once an accident starts, the sequences modeled by the event trees can result in either the prevention of core damage by system operation (as defined by the success criteria) or in the occurrence of fuel damage and the release of fission products from the core and, in some cases, from the containment. The accident reaches a successful end-point if the reactor can be maintained at a stabilized hot shutdown condition after becoming subcritical with adequate RPV water makeup as defined by the success criteria.

la
4a

Core damage prevention is accomplished by either the start of a containment heat removal system (prior to loss of containment integrity), or the maintenance of RPV water makeup (despite the loss of containment integrity).

3. PROBABILITY OF CORE DAMAGE

This section summarizes the methodology employed in the assessment of the probability of accident sequences and core damage. Human and equipment reliability models and system descriptions are used to construct system fault trees. These trees and the applicable success criteria are utilized in accident event trees to analyze the accident initiation events. The frequency of core damage is calculated either directly from the accident event trees, or indirectly by means of the containment event trees (discussed in Section 4) which are used to determine if loss of heat removal and containment integrity can lead to core damage. The methodology in assessing frequency of core damage and fission product releases is schematically illustrated in Figure 3.0-1.

3.1 ACCIDENT INITIATORS

This section describes the initiating events of the core damage accident sequences developed in Appendix C. The accident initiators are separated into two general groups, transients and loss of coolant accidents (LOCAs). Table 3.1-1 provides a summary of the accident initiators and their expected frequency of occurrence used in the Appendix C event trees.

The individual transient accident initiator frequencies were calculated from BWR plant operating experience modified to reflect BWR/6 Standard Plant Design features. The data base represents 100 plant-years of experience. The only exceptions are for the evaluation of the event frequencies for loss of offsite power and inadvertent open safety/relief valve. These two frequencies were obtained from a data base study and reliability analysis, respectively, which provide the basis for estimating

3. PROBABILITY OF CORE DAMAGE

This section summarizes the methodology employed in the assessment of the probability of accident sequences and core damage. Human and equipment reliability models and system descriptions are used to construct system fault trees. These trees and the applicable success criteria are utilized in accident event trees to analyze the accident initiation events. The frequency of core damage is calculated either directly from the accident event trees, or indirectly by means of the containment event trees (discussed in Section 4) which are used to determine if loss of heat removal and containment integrity can lead to core damage. The methodology in assessing frequency of core damage and fission product releases is schematically illustrated in Figure 3.0-1.

3.1 ACCIDENT INITIATORS

This section describes the initiating events of the core damage accident sequences developed in Appendix C. The accident initiators are separated into two general groups, transients and loss of coolant accidents (LOCAs). Table 3.1-1 provides a summary of the accident initiators and their expected frequency of occurrence used in the Appendix C event trees.

The individual transient accident initiator frequencies were calculated from BWR plant operating experience modified to reflect BWR/6 Standard Plant Design features. The data base represents 100 plant-years of experience. The only exceptions are for the evaluation of the event frequencies for loss of offsite power and inadvertent open safety/relief valve. These two frequencies were obtained from a data base study and reliability analysis, respectively, which provide the basis for estimating

3.1 ACCIDENT INITIATORS (Continued)

these frequencies (Appendices A.4 and A.6). The assessed IORV frequency is based on the Standard Plant design. A detailed breakdown of the calculated transient frequencies including the differences between current operating plant frequencies and BWR/6 Standard Plant frequencies is given in Appendix A.1.

The Reactor Safety Study, WASH-1400, (Reference 3.1-1) provided the primary basis for the LOCA initiation frequencies given in Table 3.1-1. These WASH-1400 LOCA event frequencies have been verified as applicable to the BWR/6 Standard Plant PRA. A more detailed description of the analysis basis is provided in Appendix A.1.2.

3.1.1 References

3.1-1 Reactor Safety Study, "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," USNRC Report WASH-1400, October 1975.

3.2.2.5 Interdependencies (Continued)

3.2.2.6 External Causes

The BWR/6 PRA does not evaluate risk due to sabotage, seismic events, fire, external floods, tornadoes, airplane crashes and other external events. However, it should be noted that nuclear industry and regulatory design and operational practices provide significant protection against such events. Furthermore, it should be noted that in evaluating the risk due to external events, site specific factors (e.g., presence of dams, earthquake faults, and airports) are important and often controlling. No attempt was made to identify such factors for the site selected for this PRA. Finally it should be noted that realistic evaluation of public risk due to external events is quite complex since such events pose significant public risk independent of the presence of a nuclear power plant.

3.2.3 Human Error Prediction

The guide for evaluation of human performance in this risk analysis has been the "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application," (NUREG/CR-1278) (Reference 3.2-2). Appendix A.5 summarizes the implementation of NUREG/CR-1278 as applicable to this study.

3.4 FREQUENCY OF CORE DAMAGE (Continued)

The reasons for this distribution are the large diversity and redundancy of RPV makeup systems available for cases other than loss of off-site power (LOOP). For LOOP events, the common mode failure of all three diesel generators causes a loss of on-site power which decreases the number of available RPV makeup systems.

The contribution of loss of heat removal followed by core damage (i.e., class II) is small.

4.4 CONTAINMENT EVENT TREES

For each accident sequence, the containment tree classifies all probaole outcomes in terms of release sequences. The construction of these trees is similar to the accident event trees discussed in Section 3.3.3. Figure 4.4-1 provides an example of a containment event tree.

1
3c,
42

4.5 CONSOLIDATED RELEASE SEQUENCES

As stated in Section 4.4 the containment event trees define the frequency of release sequences. The time sequence and core damage history associated with each release sequence are represented by the appropriate accident class. Given the accident, each release sequence has four important parameters: (1) frequency of the sequence, (2) the release path associated with the sequence, (3) the associated accident class, and (4) the timing of the release.

This combination of release sequence and accident class is defined as a "release category." Consequently, the CORRAL and CRAC code inputs are also determined by these release categories.

Table 4.5-1 provides an example of release categories for Class I_T. This format represents all possible release categories for accident classes I_L, I_T and III where each class matches the applicable containment event trees in Table 4.4-1. This provides an example of how release sequences are consolidated. Each release category is coded and represented by the predominate release sequence within this category. For example, an accident which includes suppression pool scrubbing throughout the sequence is identified as I-T-I3.

. Further efficiency is accomplished by combining small frequency release categories with similar higher frequency release categories. Consequently, 15 release categories were input to the CORRAL and CRAC codes for the calculation of consequences (see Table 4.5-2).

Table 4.5-2

LIST OF CONSOLIDATED RELEASE CATEGORIES
INPUT FOR CORRAL AND CRAC RUNS

Class	Name	Base category	Other categories
I_T	Transients	L3	E2, E3, I2, I3 and L2 + (El and Ll)*
I_{SB}	SB or IB LOCA transient	L3	El, E3 and Ll
I_{LB}	LB LOCA transient	L3	Combined with I_{SB}
II_T	Loss of Heat Removal following a drywell LOCA	B3	Combined with B3
II_L	Loss of Heat Remova: following a drywell LOCA	B3	Combined with B3
II_A	Loss of Heat Removal with faster containment pressurization	B3	Combined with B3
III	ATWS w/o RPV makeup	Added to I_T (negligible frequency)	
IV	ATWS w/o SLC ınjection	F3	Combined with F3
V	Ex-Drywell LOCA transient	Added to I-SB-El (negligible frequency)	
VI	Containment LOCA causes loss of containment integrity	Processed via II_A and I-SB-El (negligible frequency)	

Coding example: I-SB-L3, i.e., Class I small break LOCA category (continuous suppression pool scrubbing and late loss of containment integrity)

*Combined with class I-SB-El and Ll

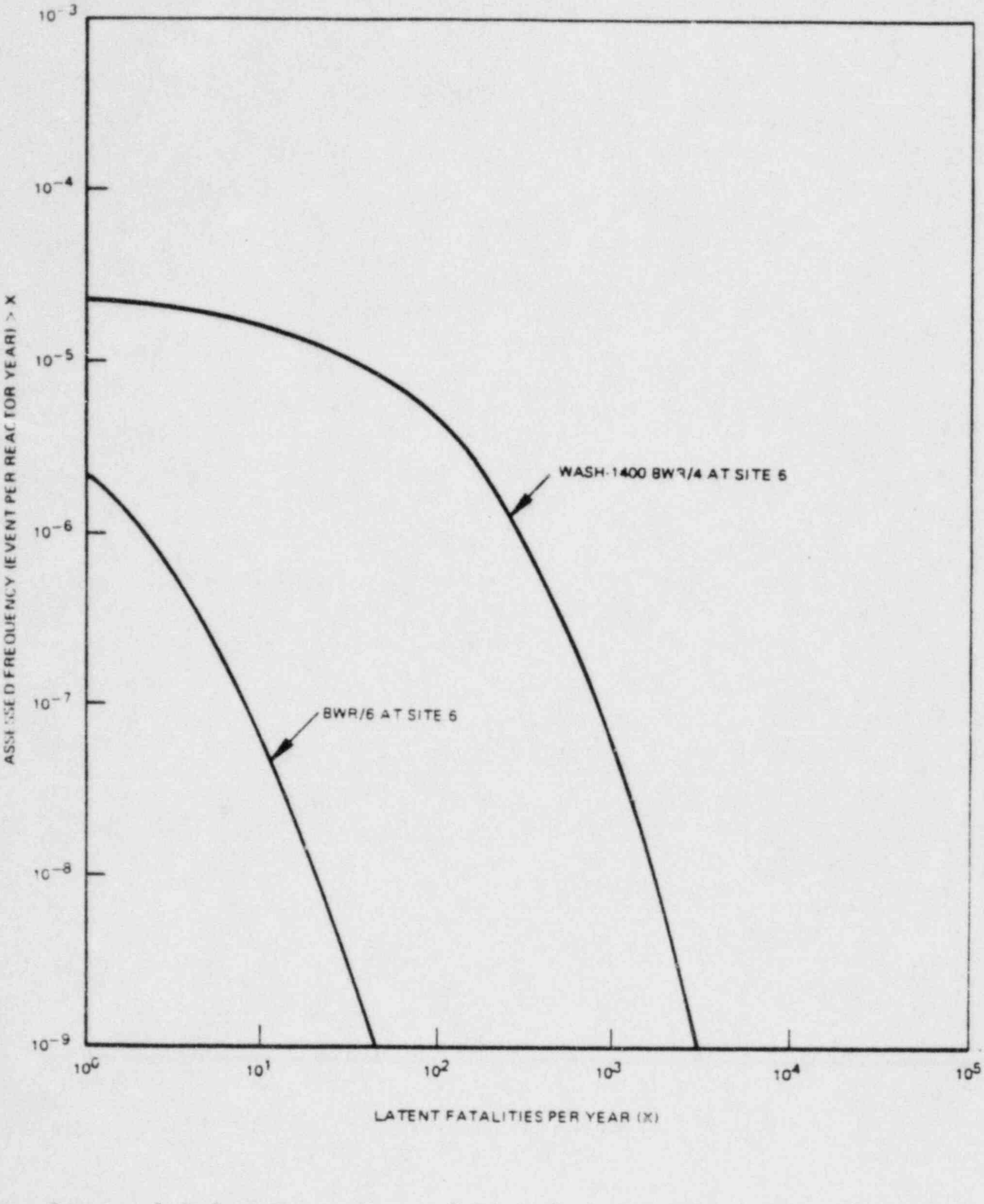

Figure 7.1-2. Comparison of Risk for the WASH-1400 BWR/4 and BWR/6

7.2 COMPARISON WITH WASH-1400

The Reactor Safety Study (WASH-1400) and the BWR/6 PRA are similar studies in that they both analyze the risk to the public from nuclear power operation. The methodology used is basically the same (probabilistic event/fault tree analysis) and the results are presented in the same manner (complimentary cumulative frequency functions of offsite consequences).

Table 7.2-1 compares the frequency of core damage of both studies. While both employed similar quantification techniques, the details of the two analyses are substantially different. The BWR/6 and the RSS BWR/4 have significant design differences. Also, the BWR/6 assessment is more comprehensive than the RSS. In many cases, the BWR/6 fault trees analyze more components and more potential failure modes. Most BWR/6 event trees contain more details allowing for more interactions. A larger number of accident classes and release categories are modeled for BWR/6. Furthermore, the BWR/6 analyses contain a major ATWS sequence which was not included in the RSS. In addition, the BWR/6 PRA includes an updated assessment of initiating event frequency based on operating experience, revised component failure probabilities justified by design differences and additional data, and more realistic success criteria than were available for the RSS.

The net effect of these differences is that the estimated BWR/6 standard plant frequency of core damage per reactor year is lower by a factor of eight, compared to the estimated RSS mean value.

A more realistic treatment of fission product transport modeling relative to the RSS is included in the BWR/6 PRA. Credit was taken for in-vessel retention and for fission product scrubbing

7.2 COMPARISON WITH WASH-1400 (Continued)

in a saturated suppression pool. In the RSS, BWR risk was evaluated for a composite of sites, which was meant to represent a composite of all BWR sites in the United States. In the BWR/6 analysis, the risk was evaluated at a specific site (RSS Site #6). The difference in risk due to the site difference is small as can be seen by comparing the curve for the WASH 1400 BWR at the composite site with the curve for the WASH-1400 BWR at Site #6 (Section 2.6).

Another difference in the evaluation of risk was the use of an updated version of the CRAC code in the BWR/6 analysis. The difference in risk due to the use of a different CRAC code was small and is shown in Appendix F.4.

Figure 7.1-2 compares the RSS and BWR/6 CCFF risk curves for latent fatalities. The risk of latent fatalities for the BWR/6 is less than the risk for the WASH-1400 BWR at Site 6 by a factor of about 55 (Table 7.2-1). This reduction is primarily due to the additional prevention and mitigation features of the BWR/6 - Mark III design.

Another measure of risk is the assessed average number of consequences (early and latent fatalities) per reactor year. The RSS provided no evaluation of average number of consequences specifically for the BWR. Only risks for the combined average for the BWR and PWR plants were provided (Reference 7.2-1). To provide a basis for comparison with the WASH-1400 BWR, the average number of consequences was estimated from the RSS BWR CCFF curves. The BWR/6 risk is lower by several orders of magnitude as shown in Table 7.2-1.

7.2.1 References

7.2-1 "Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG 75/014, U.S. Nuclear Regulatory Commission (1975).

Table 7.2-1

ESTIMATED CORE DAMAGE AND RISK COMPARISON

		Risk	
Event	Assessed Frequency of Event Per Reactor Year	Early Fatalities Per Reactor Year	Latent[b] Fatalities Per Reactor Year
I. CORE DAMAGE			
RSS BWR/4 Mark I @ composite site	$\sim 4x10^{-5}$	$\sim 1x10^{-5}$[a]	$\sim 5x10^{-2}$[a]
RSS BWR/4 Mark I @ site #6[c]	$\sim 4x10^{-5}$	$1.2x10^{-6}$	$1.1x10^{-2}$
BWR/6 Mark III @ site #6[c]	$5x10^{-6}$	0	$2x10^{-4}$
II. U.S. NATURAL BACKGROUND RADIATION	Continuous	0	814

[a] With WASH-1400 Methods (calculated from the reported curves).

[b] The total accident-caused fatalities over the lifetime of the exposed population or the calculated excess cancers in the same population from one year of background radiation.

[c] Computed with the GE CRAC Code.

7.3 COMPARISON TO OTHER RISKS

The risk associated with reactor accidents can also be compared with the average natural background exposure in the United States, by estimating the mean value of lifetime cancer fatalities due to an average background dose of 100 millirem per person per year. Man-Rem exposure from background radiation is calculated for the same 500 mile radius area and the same population demography (81.4 million people) used for the postulated accident. The US NRC estimated excess lifetime death rate of 100 cancer fatalities/ million person-rems is used for this analysis (Reference 7.3-1) The latent fatalities risk associated with BWR/4 or BWR/6 reactors is significantly lower than the corresponding background radiation risk by four and seven orders of magnitude, respectively (Table 7.2-1).

Another comparison is made to natural and man-made hazards, based on statistics for the frequency of these hazards in the USA as displayed in Figures 7.3-1 and 7.3-2 (Ref. 7.3-2). These figures compare the actuarial or estimated average U.S. frequency of fatalities per year caused by natural or manmade hazards (adjusted to site 6 population) to the assessed frequency of latent fatalities per year attributed to hypothetical nuclear accidents. For example, on the average there is about one tornado and four aviation accidents per year which cause at least ten fatalities each. This is compared to the assessed frequency of less than $1x10^{-6}$ per year of reactor accidents with one or more fatalities. Thus the risk from nuclear accidents at site six is smaller by a factor of more than a million than the risk associated with most natural and man-made hazards. The comparison in this case is not exact since fatalities as a result of these hazards are immediate and their frequency is substantiated by experience, whereas the reactor curves result from a best estimate calculation of potential latent fatalities.

7.3.1 References

7.3-1 "Instruction Concerning Risks from Occupational Radiation Exposure," Regulatory Guide 8.29, U.S. Nuclear Regulatory Commission (1981), Tables 1 and 6.

7.3-2 A. Coppola, R. E. Hall, "A Risk Comparison," NUREG/CR-1916, U.S. Nuclear Regulatory Commission (1981).

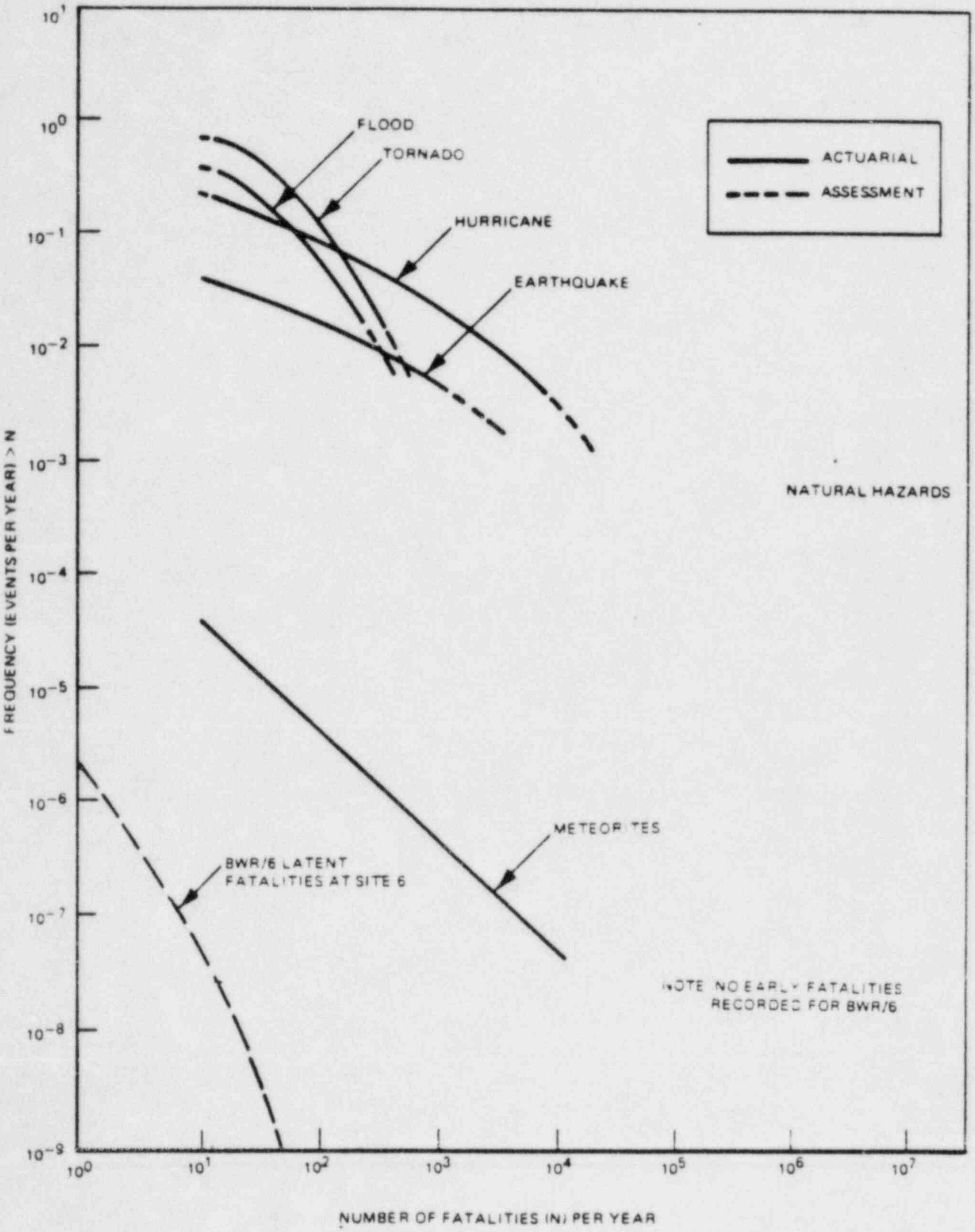

Figure 7.3-1. Risk Comparison Between Natural Hazards and BWR/6

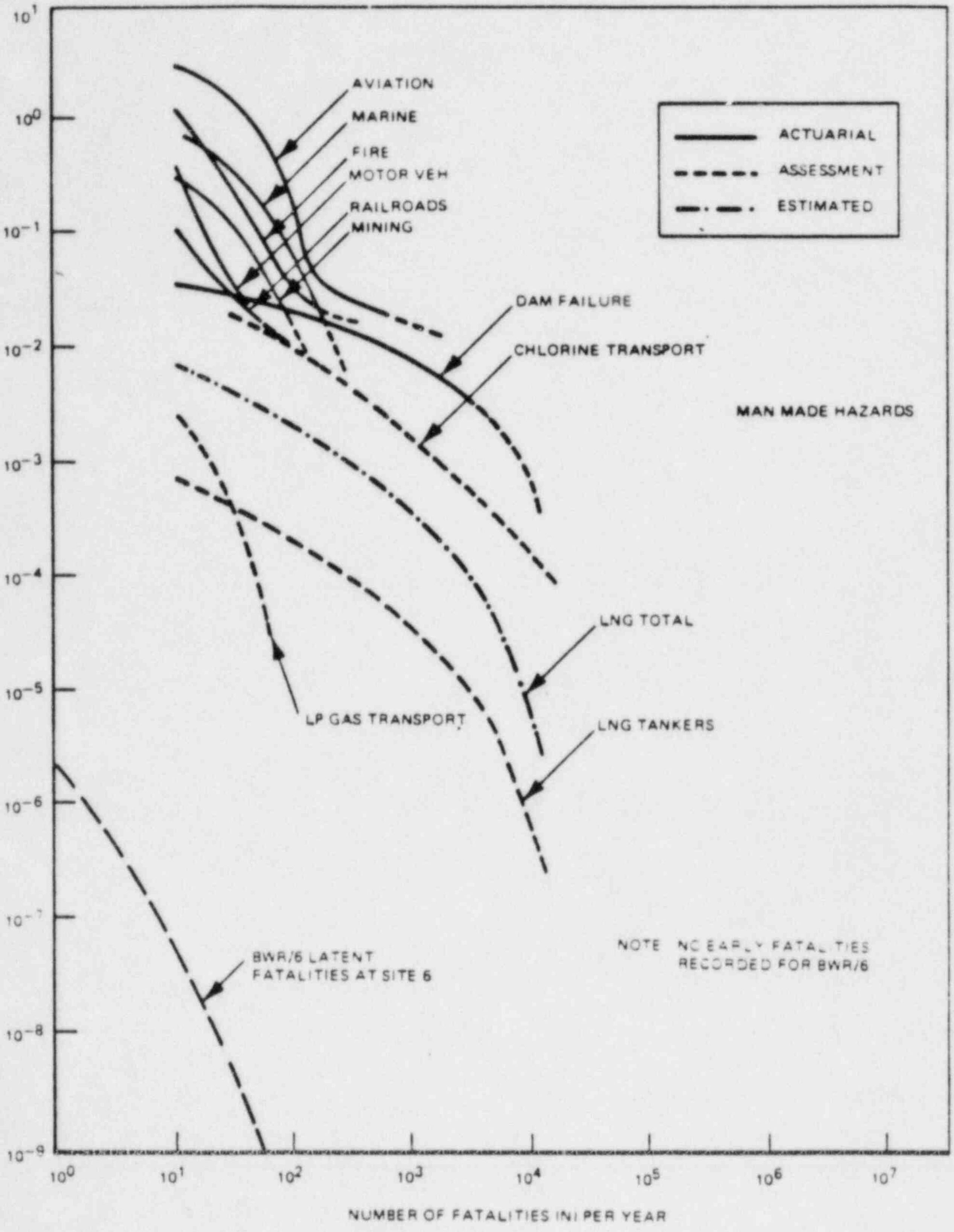

Figure 7.3-2. Risk Comparison Between Man Made Hazards and BWR/6

7.4 OVERVIEW OF CONDITIONS AND LIMITATIONS

This study is generally based on state-of-the-art methodology and does not present an innovative approach to risk analysis. All PRA studies are subject to certain limitations. The major limitations applicable to this PRA study are described and discussed below.

7.4.1 Plant and Data

The BWR/6 PRA addresses a standard plant at a selected site with a representative grid for that site. The analysis is based on NSSS and BOP design drawings that characterize the BWR/6 standard plant, and on design modifications to the standard plant. Human, component and system failure probabilities are based primarily on commonly used generic data from operating experience and other nuclear sources. Mean values or values judged to represent mean values were used throughout the analysis. It is recognized that the analysis of a specific plant design at an actual site may produce different results.

7.4.2 Scope

This PRA study addresses the potential risk to the public from nuclear accidents during operation. The risk associated with other activities such as normal operation or fuel handling, storage and disposal is not treated. The risk associated with external events, such as earthquake, fire, flood, aircraft crash or sabotage is not considered, except to the extent that they are included in the data base for the frequency of loss of off-site power. Human error models include errors resulting from operator failure to act, as directed by procedures, as a functional part of the system. Inadvertent scram due to human error

7.4.2 Scope (Continued)

and instrument miscalibration are included. Human failure to follow maintenance or surveillance test tasks are assessed to have an insignificant impact on risk and are excluded.

The analysis is based on the BWR experience and statistical data accumulated over the last 20 years and on the assessed probability of unanticipated accidents (such as ATWS). Dependent (common cause) failures are similarly addressed. All known interactions and interdependencies among components and/or systems are rigorously treated. A limited attempt was also made to discover additional second order common cause failures. These failures were judged to be inconsequential, because of the numerous safety precautions and features already incorporated in the design.

7.4.3 Methodology

Delayed or partial water injection success is conservatively treated. The accident sequence analysis ends if the reactor is brought to a stable hot standby condition. If core damage starts, the accident is assumed to proceed to a "full" core damage, loss of containment integrity and fission product release, regardless of the potential for system recovery.

Core damage and consequence analyses generally follow the present state-of-the-art methods but include suppression pool scrubbing and in-vessel retention factors. Fission product source term and transport analyses are based on deterministic computer code output, supplemented in a few cases with some extrapolations to provide the necessary output. Conservatively, no credit is

7.4.3 Methodology (Continued)

taken for fission product retention within the secondary containment. The consequence analysis is based on the updated version of the WASH-1400 analysis.

7.4.4 Uncertainty

The purpose of this PRA study is to assess the public risk associated with BWR/6 accidents. Another benefit out of this study is the ability to assess the effectiveness of preventive and mitigative features of the design. Because of the complexity of the analysis and the above conditions and limitations it is difficult to state the results in precise absolute values.

The risk results of this and all other PRAs are subject to uncertainty. This uncertainty is inherent in the failure rate data and in the modeling of systems and human response, as well as the physical processes that follow degraded core conditions. The overall uncertainty is judged to be about a factor of 50 (in either direction) at the 90% confidence level based on other BWR PRAs. However, this risk is so small relative to natural and man-made hazards that this uncertainty is inconsequential.

A nuclear plant PRA is a candid analysis of extremely rare events. It should not be used out of context to assign a degree of reality to the analyzed accidents beyond that implied by the assessed frequency of consequences.

7.5 CONCLUSIONS

This BWR/6 PRA is a best estimate analysis of the frequency of potential accidents and their consequences. The low frequency of core damage results from the GE safety approach of providing system capabilities that extend beyond regulatory requirements. Specifically, the diversity of multiple low and high pressure systems for core cooling and the variety of containment heat removal modes prevent core damage and subsequent fission product releases. The lack of early fatalities associated with the postulated accidents can be attributed to the BWR/6 Mark III inherent mitigative features which maintain containment function, even for postulated severe accidents, thereby limiting fission product releases. The low risk (latent fatalities) can be attributed to both BWR accident prevention and mitigation capabilities.

A number of general inferences can be drawn from this and related studies. First, the assessed frequency of core damage and risk for the BWR/4 and BWR/6 are substantially lower than the corresponding values for major natural and man-made hazards (Figures 7.3-1 and 2). Second, the risk due to exposure to the average U.S. natural background radiation is substantially larger than the risk associated with these BWR plant accidents (Table 7.1-2). Thus, this study quantifies the effectiveness of existing designs, industry practices and regulatory requirements. Third, the reduction in early and latent fatality risk for the BWR/6 relative to the RSS BWR/4 results quantifies the benefits resulting from the evolution of the design over the years and the plant improvements that are incorporated in this PRA.

Finally, from this study it is concluded that the risk associated with the standard BWR/6, in both a relative and an absolute sense, is sufficiently low and that additional design changes are not appropriate.

APPENDIX A: INPUT DATA FOR PROBABILISTIC EVALUATION

CONTENTS

A.1 ACCIDENT INITIATORS

The initiating events used in the Appendix C event trees (which model core damage accident sequences) are discussed in this section in the approximate order of their respective event frequency. Transients are discussed in Section A.1.1, f.llowed by the Loss of Coolant Accidents (pipe breaks) in Section A.1.2. The discussion of rupture of the reactor pressure vessel as an initiating event is presented in Section A.1.3.

A.5 HUMAN ERROR PREDICTION

A.5.1 Introduction

The two ways in which human error can be included in a PRA are:

(1) The human is included in the fault tree or event tree structure just as if he were a piece of hardware whose failure or degraded performance causes loss of the system function.

(2) The human or several humans perform a series of tasks in conducting surveillance tests, repairs and other maintenance. Failure to perform these tasks correctly can result in the unavailability or malfunction of safety or safety related equipment on demand.

The human as a functional element in the fault or event tree is the principal application of human error probability (HEP) in the BWR/6 PRA. The reasons for this are discussed in the following paragraphs.

A.5.2 General Discussion

The source for HEP practice and application in the BWR/6 PRA is "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," by A.D. Swain and H.E. Guttmann is issued as NUREG/CR-1278, April 1980 (Reference A.5-1). Summary material from that document and additional material from other sources are included in the PRA. In general, human errors both of commission and omission are expected to be reduced by operator training, C.1.3.4 Symbols Used in Containment Event Trees (Continued)

E_I is the probability that following a loss of primary containment integrity and/or suppression pool saturation, no suppression pool water is injected into the RPV.

E_N is the probability that following a Class IV ATWS event, the throttled water level in the RPV will not be maintained to prevent a core melt.

E_O is the probability that following a loss of primary containment integrity and/or suppression pool saturation, no RPV makeup water is injected from sources external to the containment, such as the condensate storage tank (CST) because of equipment failure or human errors.

E_T is the probability that following a Class IV ATWS event, the operator will not temporarily reduce the RPV continuous blowdown into the containment by throttling the RPV makeup and lowering the RPV water level below the top of the active fuel.

W_N is the probability that following a Class IV ATWS event and a RPV blowdown to the containment, adequate containment heat removal is not maintained, because of equipment failure or human errors.

C.1.4 Event Tree Example

For illustration purposes, an example event tree for the reactor shutdown initiating event is given in Figure C.1-2. The initiating event is given as the first branch in the far left column of

1a
3a
4a
Re

C.1.4 Event Tree Example (Continued)

the event tree. The initiating event name, symbol, and frequency of occurrence (events/year), are provided at the top of the column. The tree is developed further by identifying the system functions required for successful termination of the event in the approximate chronological order of occurrence. The success and failure states of each system function are given as branches in the tree with the top branch representing success and the bottom branch failure. If a prior system function directly leads to a success or failure during the accident sequence, analysis of the remaining system functions is not necessary. The information given at the top of the column for each system function is the same as that given in the initiating event frequency column with the exception that the frequency value is replaced by a conditional failure probability value for the system function.

The accident sequences (event tree branches) terminate at the far right column. The sequence symbol, classification of effect, and frequency of occurrence is given for each tree branch. The classification of a sequence results either in successful termination (designated by "OK"), a core damage or loss of containment heat removal (designated by the containment event name, such as, CT2T, where the sequence is developed further) or a sequence which is developed further in another accident event tree (e.g., the sequence, $T_M F_O$, representing unplanned reactor shutdown is included in the turbine trip event tree). The frequency of each branch is given by the product of the initiating event frequency and conditional probabilities of the system functions in the accident sequence.

APPENDIX D: FAULT TREES

The event trees in Appendix C are used to identify the key system functions that are involved in each accident sequence. Appendix D presents the Boolean models of combinations of components, systems or functions used to provide probabilistic values for the event trees. Boolean combination is necessary in those instances where there are common dependencies among systems or functions. Examples of such dependencies are electric power, instrument air, common sensors, service water and the requirement that maintenance on one safety system be carried out exclusive of maintenance on certain other safety systems.

In Appendix C, each branch point (or node) in the event trees has a conditional probability of occurrence and a complementary probability of not occurring. Appendix D provides the basic unavailability value for the derivation of the fault tree probabilities, usually from (or involving) the basic failure rate data in Appendix A. Thus, to derive the value on the event trees, basic failure rate data for components, logic and human action are applied to the fault tree models, incorporating appropriate operating time and test intervals to obtain key system or function availabilities. The system or function availability is then tailored to the individual accident sequence event trees, taking into account interdependencies and the specific conditions of each event.

This appendix is organized in two sections. Section D.1 contains functional fault trees which model the interaction of several systems to provide reactor coolant injection. Section D.2 provides system level fault trees for the 14 systems that were modelled and analyzed. The fault trees utilize symbols consistent with the current state-of-the-art (Reference D.1-1).

D.1 FUNCTIONAL FAULT TREES

Reactor coolant injection is essential to successful termination of all accident sequences. Successful injection may be achieved by any of eleven pumps in several systems, either at high or low reactor pressure (Section 3.3.1). Figure D.1-1 is a functional fault tree depicting the coolant injection function. The computer model for this tree provides the means for evaluating the interaction of any interdependencies between the systems involved.

The systems involved in providing or supporting reactor coolant injection are the following:

1. Condensate and Feedwater
2. Reactor Core Injection Cooling (RCIC)
3. High Pressure Core Spray (HPCS)
4. Automatic Depressurization (ADS)
5. Low Pressure Core Spray (LPCS)
6. Low Pressure Coolant Injection (LPCI)
7. Control Rod Drive (CRD)
8. Essential Service Water (ESW)
9. Electric Power

Referring to Figure D.1-1, the loss of coolant injection (RXINJECT) requires the loss of all high pressure systems (HPI) and all low pressure systems (LPI). High pressure systems are driven by

D.1 FUNCTIONAL FAULT TREES (Continued)

electric motors (HPCS and CRD) or steam turbines (FW and RCIC). Motor driven systems require electric power. Turbine driven systems require the reactor to be at a pressure to provide sufficient motive steam. Low pressure systems (LPCS, LPCI, and condensate pumps) require the reactor to be at a pressure consistent with the driving capability of the pumps. The RPV can be depressurized to access the low pressure systems. This depressurization can be accomplished either automatically (by ADS) or manually. All low pressure systems have motor driven pumps and require electric power.

1a
3a
4a

D.1.1 References

D.1-1 NUREG-0492, "Fault Tree Handbook," U. S. Nuclear Regulatory Commission, January 1981.

D.2 SYSTEM FAULT TREES

System fault trees are used to develop the Boolean computer models which evaluate interactions within the system and interdependence with supporting systems. The system fault trees with the corresponding system unavailabilities are listed in Table D.2-1.

The Boolean models utilize components and human action failure probabilities to compute system unavailability upon demand. Human action failure probabilities are treated in Appendix A.5. Standby component failure rates are discussed in Appendix A.2 and are applied either on a per-demand basis or on an elapsed time basis (time since the last surveillance test), whichever is appropriate in the sequence of events. For some components (e.g., diesel generators), the data base provides the failure probability directly and the component failure probability (P_f) upon demand is on a "per demand" basis, regardless of the elapsed time since the last surveillance test. For components in standby status, the following relationship is used when the input data are elapsed time failure rate.

$$P_f = 1\text{-exp}\,\frac{-\lambda\theta}{2}\ ,$$

where:

P_f is the probability of a component failure on demand,

λ is the failure rate, and

θ is the scheduled elapsed time between tests.

APPENDIX F: DESCRIPTION OF COMPUTER MODELS AND METHODS

This Appendix describes the principal computer models and methods used in the BWR/6 Standard Plant PRA. Section F.1 describes the WAM series of computer codes and their use to obtain minimum cut sets of system unavailability upon demand which were used in the event and fault trees in Appendices C and D. Section F.2 describes the MARCH code modeling of core meltdown phenomena. Section F.3 describes the modeling of fission product transport as performed by the CORRAL code. The consequence evaluation is performed by the CRAC code as described in Section F.4.

F.1 THE WAM COMPUTER CODES

F.1.1 Introduction

The WAM series of computer programs provides the capability of conducting a probabilistic and qualitative evaluation of systems modeled with Boolean Algebra (References F.1-1 and F.1-2). This Appendix documents the use of the WAM programs and references the instructions necessary for executing the programs (Reference F.1-3).

The two WAM codes identified in this report complement each other in the probabilistic and quantitative analysis of systems. The WAMBM01C and WAMCT01C codes evaluate systems modeled with Boolean algebra.

F.1.2 Application

The computer code WAMBM01C evaluates probabilistically, systems modeled with Boolean algebra. These models take the form of event trees, fault trees or simply a Boolean expression. The code calculates point estimate probabilities (expected values)

F.1.2 Application (Continued)

for the events of interest in the system from point estimates of the components unavailability or availability.

The computer code WAMCT01C is used for the quantitative evaluation of fault trees by obtaining the minimum cut sets (paths to system failure) and computing the unavailability of the events (gates) in the fault tree.

Details of the modeling and inputs necessary to run the codes are given in Reference F1-3. Code outputs were entered in the appropriate event and fault trees in Appendices C and D.

F.1.3 References

F.1-1 User's Guide for the WAM-BAM Computer Code, Research Project 217-2-5, F. L. Leverenz, H. Kirch, Science Applications, Inc.

F.1-2 WAMCUT, a Computer Code for Fault Tree Evaluation, NP-803, Research Project 767-1, F. L. Leverenz, H. Kirch, Science Applications.

F.1-3 NEDE 25359, "User Manual for Engineering Computer Programs," R. T. Earle, November, 1980.

F.2 CORE DAMAGE AND CONTAINMENT RESPONSE

This section provides a description of the analyses performed to evaluate the response of the containment during various core melt scenarios. Presented in the following sections are: (1) an overview of the method of analysis, (2) a description of the models used for these analyses, and (3) a discussion of the results.

F.2.1 Method Description

MARCH (Reference F.2-1), a computer code package developed by Battelle Columbus Laboratories, was used to analyze the thermal-hydraulic response of the reactor pressure vessel (RPV) and containment following core melt accidents. This code consists of a main routine MARCH and six major subroutines referred to as INITIAL, BOIL, HEAD, HOTDROP, INTER, and MACE. Each subroutine performs analysis for different time domains and compartments as described in the following:

(1) INITIAL performs calculations of the RPV blowdown into the containment,

(2) BOIL determines the RPV system response, melting and slumping of the core into lower plenum and metal-water reaction in the vessel

(3) HEAD determines the interaction of corium with the RPV bottom head and the time of loss of RPV integrity following core slump.

(4) HOTDROP determines interaction of the corium with water in the reactor cavity following melt-through of the vessel,

F.2.1 Method Description (Continued)

(5) INTER determines interaction of the corium with the concrete containment floor, and,

(6) MACE determines the containment response throughout the accident.

These subroutines are called by the main routine MARCH and communicate with each other in the manner shown in Figure F.2.1-1.

F.4 CONSEQUENCE ANALYSIS

This section describes the use of the CRAC code for calculation of the potential radiological consequences of the accident sequences described in Section 3.3.

F.4.1 CRAC Code

Evaluation of the potential radiological consequences was made using a computer code which is an adaptation of the CRAC (Calculation of Reactor Accident Consequences) computer code. Section 6.1 describes the CRAC code model and calculational procedure.

F.3.1 Fission Product Release From the Core

Fission product release from the core is divided into three release periods: gap release, melt release, and vaporization release. During the gap release period fission products are released to the reactor pressure vessel from the start of fuel rod perforation until the melt release begins.

G.11 CONCLUSIONS

From the above discussion and results in this section, the main conclusions are summarized as follows:

1. The external pressure-carrying capability of the drywell including its head is significantly higher than the internal pressure-carrying capability of the containment vessel. The drywell and the suppression pool structures are areas of the maximum pressure-carrying capability in the containment structural system.

2. In case of a static overpressurization the most probable location for loss of containment integrity is high above the suppression pool in the dome region. Such failure would leave the suppression pool intact. Containment dome failure will not fail the drywell.

3. The structural integrity of the drywell and the suppression pool will be maintained for all static overpressurization events. The pressure-carrying capabilities for the primary containment vessel and ECCS and RCIC suction lines submerged in the pool are higher than that of the containment dome.

4. In certain instances, a global hydrogen detonation would produce small shear cracks in the drywell structure but most of the fission products are directed to the suppression pool through the SRV discharge lines.

H.1 INTRODUCTION

A containment failure mechanism which was proposed in WASH-1400 was a steam explosion within the reactor pressure vessel when molten core debris is assumed to drop into the lower plenum. (Reference H.1-1) This explosive interaction was conceived to propel a slug of coolant and core debris against the upper reactor vessel head with sufficient energy to fail the reactor vessel and the resultant missile was conceived to fail the drywell head and the containment wall upon impact. Another postulated mechanism was a steam explosion in the pedestal cavity below the vessel when the molten core debris is assumed to drop into the water collected in the pedestal upon failure of the vessel bottom head. This explosive interaction was conceived to displace the vessel from its foundation and to result in loss of drywell integrity upon impact followed by damage to the containment due to the displacement of the pipe and other structures in the containment.

A steam explosion is the shock wave created by a rapid evaporation of water and an almost instantaneous expansion of the resulting steam when water and a hot liquid, e.g., molten corium, are mixed. The sequence of events associated with a steam explosion are 1) coarse fragmentation of the molten metal, 2) fine fragmentation and mixing of the molten material and finally, 3) the explosive vaporization.

Available steam explosion models predict that molten core debris and water could present an explosive system, i.e. the principal question is not whether steam explosions can occur. Rather the principal considerations are the amount of material involved, the manner in which the hot and cold fluids intermix, and the transmission mechanism whereby the vaporization work is transmitted to the reactor pressure vessel.

H.1 INTRODUCTION (Continued)

In this appendix, the analyses used in WASH-1400 are reviewed in terms of the basic physical processes involved in the model and those required for RPV failure. Next the specific structural configurations of the BWR/6 Standard Plant are discussed paying particular attention to their influence on the establishment of initial conditions for explosive interactions and the transmission of the expansion work. This is followed by a detailed discussion of the relevant phenomena including pertinent experimental results, and these basic considerations are then applied to the available large scale experimental results performed at Sandia National Laboratory. Finally, the same basic considerations are applied to the BWR/6 Standard Plant to assess the potential for establishing the necessary initial conditions and for mixing the two materials on an explosive time scale. This assessment of the nature and scale of the molten metal/water interaction was carried out both for inside the RPV in the lower plenum and outside the vessel in the pedestal cavity. It is concluded from these assessments that a loss of containment or reactor pressure vessel integrity will not occur as a result of steam explosions.

H.1.1 References

H.1-1 Reactor Safety Study, WASH-1400, NUREG/750114, 1975.

H.2 STEAM EXPLOSIONS AS MODELED IN THE REACTOR SAFETY STUDY (WASH-1400)

H.2.1 <u>In-Vessel Explosion</u>

As an initial condition for the steam explosion, a degraded core state was assumed in which the core was uniformly molten and *totally separated* from the water contained in the lower plenum by the grid plate. It was considered unlikely that a partially molten core would drain into the lower plenum. Consequently, the core was assumed to collect on the grid plate and this was assumed to fail in a catastrophic manner releasing all the molten debris into the water. This failure is then postulated to cause the debris to be instantaneously fragmented to some user-specified fragment size as well as instantaneously and uniformly dispersed throughout the coolant. These conditions are assumed and not the result of mechanistic calculations describing the grid plate failure, the fragmentation process, and the mixing of the water and core material; all of which are certainly rate dependent phenomena but not represented in the WASH-1400 analyses.

Once this intimate dispersal is assumed, the thermal energy transfer is calculated by considering convection, conduction, and radiation between the core debris and water. Energy transfer results in a rapid (∿ 10 msec) pressure rise in interaction zone and this accelerates an assumed continuous, overlying liquid slug, made up of half water and half core debris, vertically upward through an open vessel in a piston-like manner as shown in Figure H.2-1. The various processes modeled are summarized in Table H.2-1 and illustrated in Figure H.2-2. Calculations are carried out for various levels of fragmentation and melt-drop times (melt addition interval). Acceleration and displacement of the postulated slug (inertial layer) continues until it impacts upon the vessel head and for some cases this is calculated to

H.2.1 In-Vessel Explosion (Continued)

occur with sufficient energy to cause the head to fail and propel it against the containment wall with the energy necessary to fail the containment. One such set of calculated results for an instantaneous melt addition and a particle size of 400 μm is shown in Figure H.2-3. Specific details of these calculations and their relation to the available experimental results will be discussed in the section on steam explosion phenomena.

Many different cases were calculated with varying particle sizes and melt-drop times, and the results showed that for either particle sizes greater than approximately 1 cm or a melt-drop time exceeding two seconds, the reactor vessel was not ruptured. Such calculational results from a highly conservative model are particularly important in light of subsequent work on mixing energies and debris release times which will be discussed later.

The analytical description used in WASH-1400 is a simplistic representation of both the specific configurations in question and the explosive phenomenon itself. These calculations misrepresent the explosive behavior in that 1) they assume that all liquid-liquid systems with a substantial temperature difference can explode, 2) no consideration is given to the rate at which the materials are brought into contact, 3) mixing is assumed to be instantaneous, uniform, and require only negligible energy, and 4) they grossly overestimate the rate of mechanical energy released by a steam explosion. Clearly, such oversimplistic analytical representations are of use in safety evaluations only if they show that even with these overwhelming conservatisms, there is still no concern for public health and safety. On the other hand, if the conclusion of such calculations is that the phenomenon does provide a considerable risk, then the basic assumptions used in the calculational model must be scrutinized

H.2.1 In-Vessel Explosion (Continued)

to discern if such a conclusion, derived from an overly simplistic model, is indeed valid. This will first be addressed in terms of the experiences with small test reactors and then with regards to the in-vessel structural components, both above and below the core, which were discussed in WASH-1400 but essentially ignored in the analysis.

H.2.2 Ex-Vessel Explosion

The possibility of steam explosions outside the vessel arise only in those instantances when there could be water in the pedestal cavity below the vessel. WASH-1400 considered the passage of molten material from inside the vessel into the water in the drywell in relatively small quantities and over a period of time. It also considered a significant fraction of the molten core dropping into the water coherently upon the meltthrough of the reactor vessel bottom head. WASH-1400 concluded, without any modeling of the metal/water interaction outside the vessel, that "for reactors enclosed in relatively large volume containments it is considered improbable that a steam explosion outside the reactor vessel would rupture the containment."

In this appendix it will be quantitatively demonstrated that WASH-1400 conclusions regarding the consequences of steam explosions outside the vessel are applicable to the BWR/6 Standard Plant with the Mark III containment system.

Table H.2-1

IN-VESSEL STEAM EXPLOSION SEQUENCE - WASH-1400

1. Uniformly molten core, totally separated from the water in the lower plenum.

2. Catastrophic collapse of the core support such that the molten core material falls into the water.

3. Rapid (instantaneous) intimate mixing of the water and core material.

4. Coherent interaction between the molten core debris and water.

5. Slug formation and accleration upward through the vessel in a piston-like manner.

6. Coherent slug impact on the vessel head.

Release

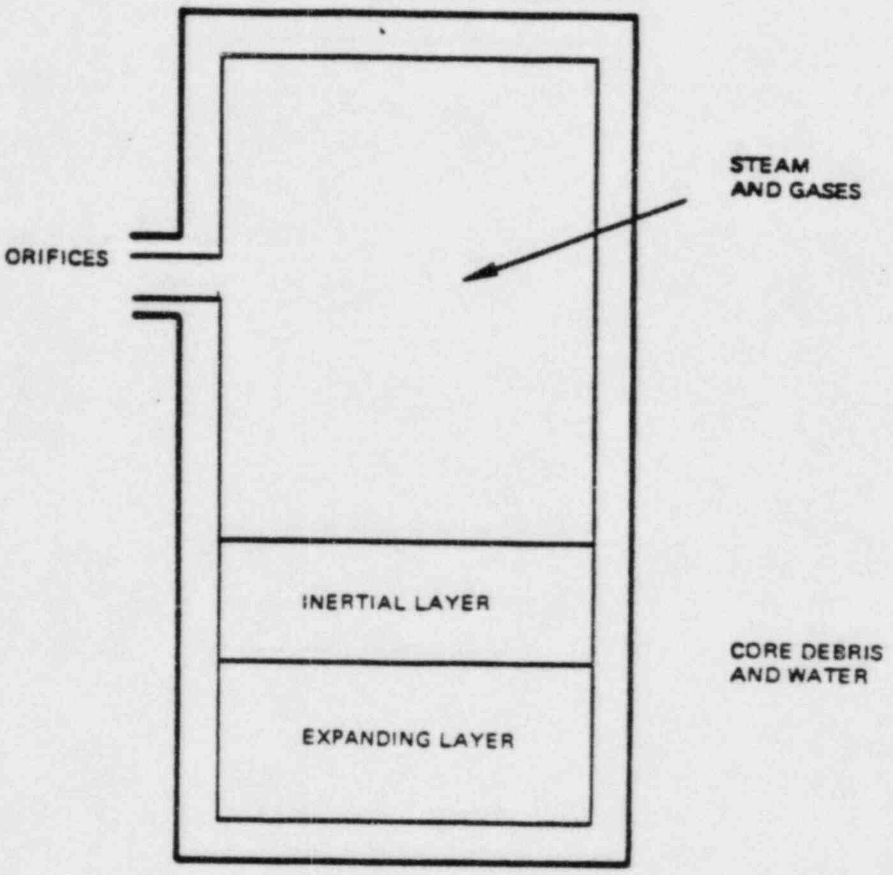

Figure H.2-1. Model Geometry Used in WASH-1400 Steam Explosion Analyses

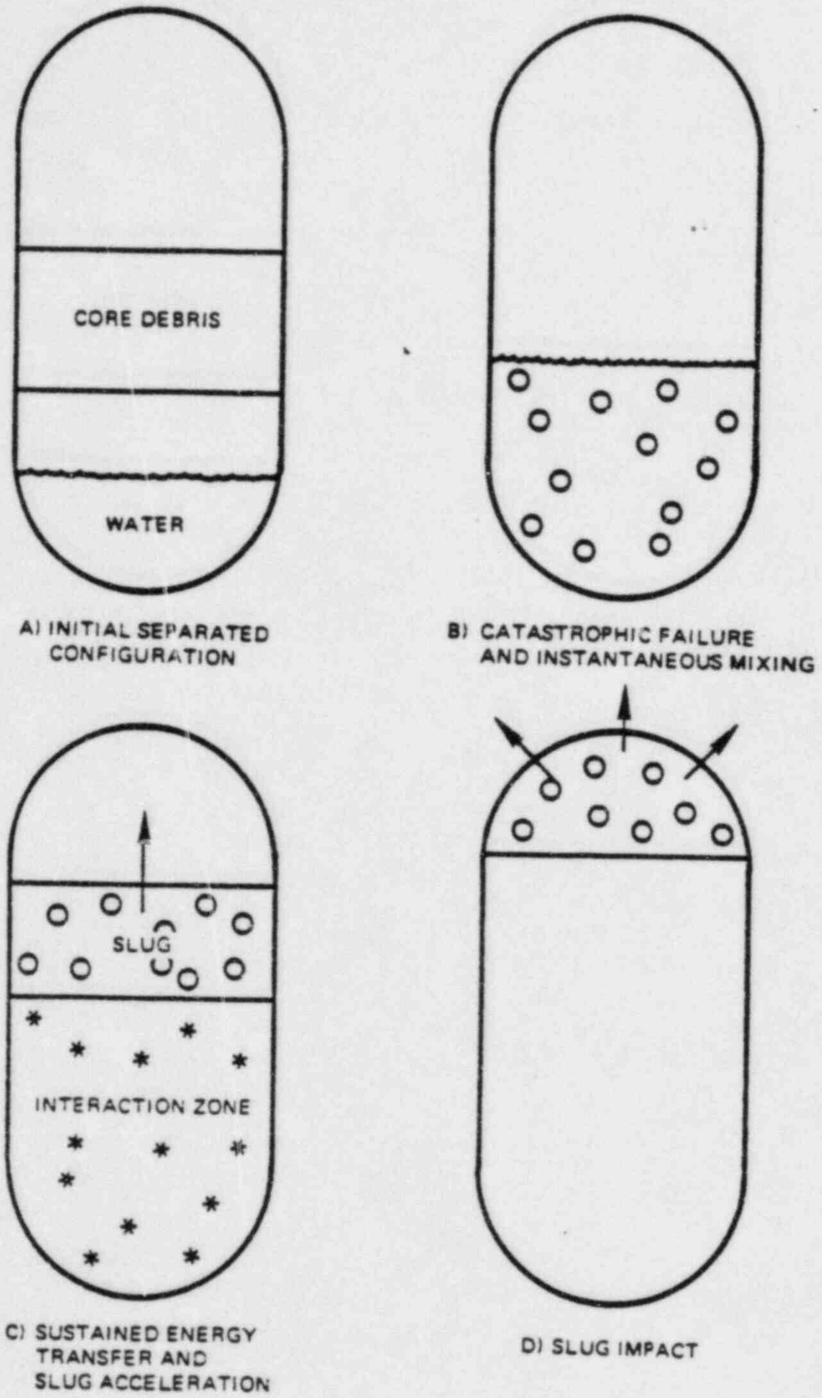
CORE DEBRIS
WATER
A) INITIAL SEPARATED CONFIGURATION
B) CATASTROPHIC FAILURE AND INSTANTANEOUS MIXING
SLUG
INTERACTION ZONE
C) SUSTAINED ENERGY TRANSFER AND SLUG ACCELERATION
D) SLUG IMPACT

Figure H.2-2. Behavior Modeled in WASH-1400

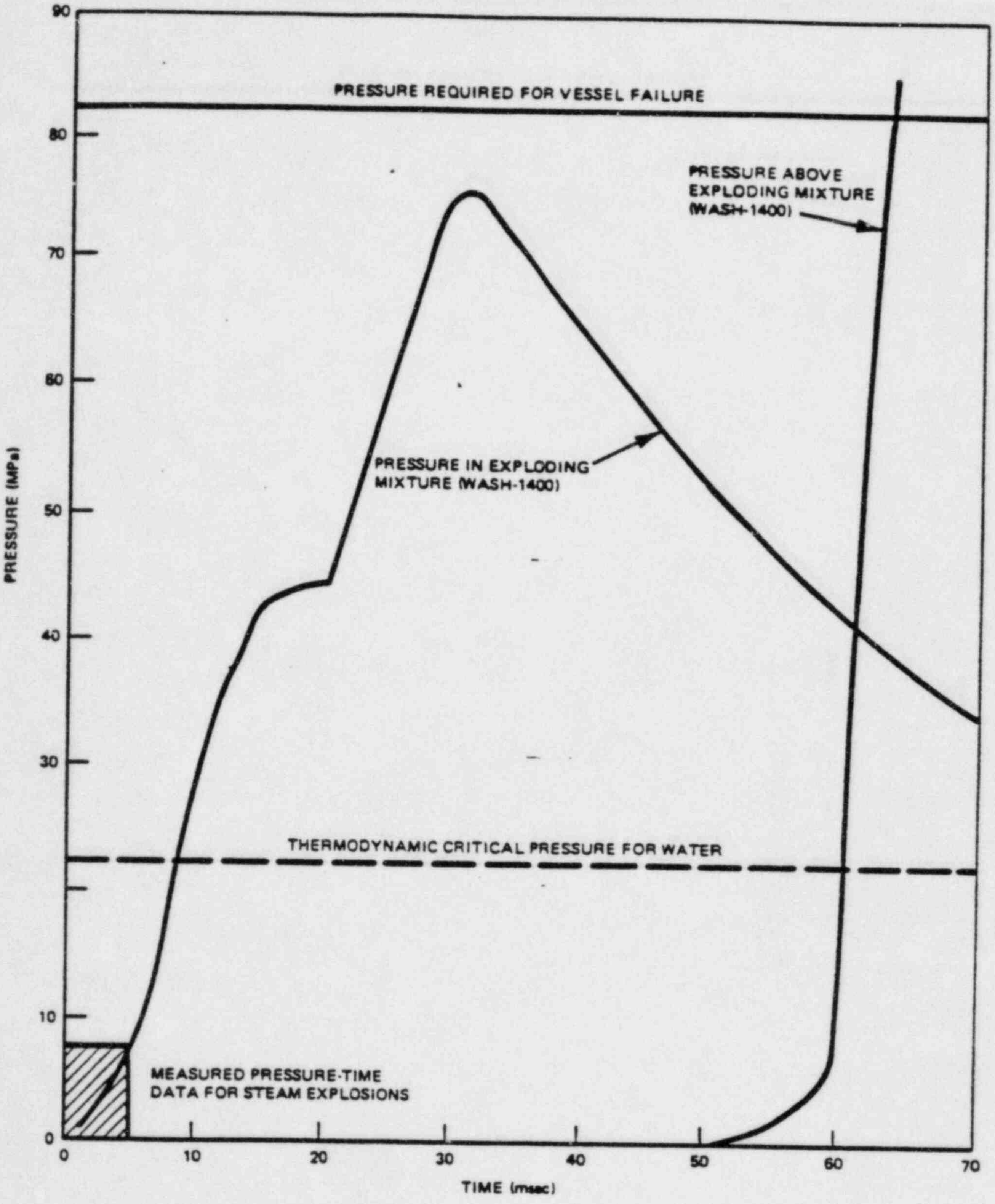

Figure H.2-3. Comparison of Predicted Pressure-Time Behavior From WASH-1400 (400 μm Particle Size) and Available Experimental Results from Steam Explosions

H.3 RELATIONSHIP TO PREVIOUS REACTOR EXPERIENCE

The conceptual steam explosion model used in WASH-1400 resulted principally from concerns generated by the low pressure BORAX and SPERT destructive experiments and the SL-1 accident (References H.3-1, H.3-2, H.3-3) Reactor conditions leading to this accident and the destructive transients in BORAX and SPERT produced a fundamentally different system than that representative of a postulated severe accident in the BWR/6 Plant. It is not only important to realize these differences, but it is essential to understand the resulting implications on the phenomenon as well. These differences and the resulting implications are:

1. All three events were produced by power excursions in which the core was driven to molten conditions in 30 msec or less. Such reactivity transients are not possible in power reactors and were neither addressed in WASH-1400 nor are they considered here.

2. For these three reactors which were fueled with uranium-aluminum alloy fuel plates clad with aluminum, the fuel and water were uniformly *premixed* and finely divided in a cold condition prior to the excursion.

3. The reactor was essentially at atmospheric pressure and water was at room temperature, hence, net vaporization was not required in the fragmentation state.

4. The SL-1 core was designed so that the reactor could be brought to criticality by the withdrawal of one control rod. In the accident this rod was rapidly withdrawn which caused a nuclear excursion with sufficient energy deposition to melt the high thermal response fuel-clad plates while in an extensively premixed state. This was also true for the BORAX and SPERT test reactors.

H.3 RELATIONSHIP TO PREVIOUS REACTOR EXPERIENCE (Continued)

5. Since the reactors were essentially at room temperature prior to the excursion, the vessels were filled with water except for a small freeboard volume at the top, i.e., a coherent overlying liquid slug was already in place.

6. The internal geometry of the vessels were very simple and open, which provides little attenuation or dispersion of any slug movement.

With these pre-transient conditions, the configuration established was essentially that assumed in WASH-1400. The essential feature of the strong reactivity transient is that it brought the fuel and clad to melting before this configuration could substantially change. Given these particular characteristics, a slug impact following a steam explosion within the core would indeed be the expected chain of events. *However, this is fundamentally different than an initially separated system of high temperature molten core material and saturated water existing at an elevated pressure with substantial internal structure to prevent catastrophic collapse, intimate mixing, and slug formation.*

H.3.1 References

H.3-1 J. R. Deitrich, "Experimental Investigation of the Self-Limitation of Power During Reactivity Transients in a Subcooled Water-Moderator Reactor-BORAX-1 Experiments, 1954," AECD-3668, 1965.

H.3-2 R. W. Miller, A. Sola and R. K. McCardell, Report of the SPERT-I: Destructive Test Program on an Aluminum, Plate-Type, Water-Moderator Reactor," IDO-16883, 1964.

H.3-3 SL-1 Project, "Final Report of the SL-1 Recovery Operations," IDO-19311, 1962.

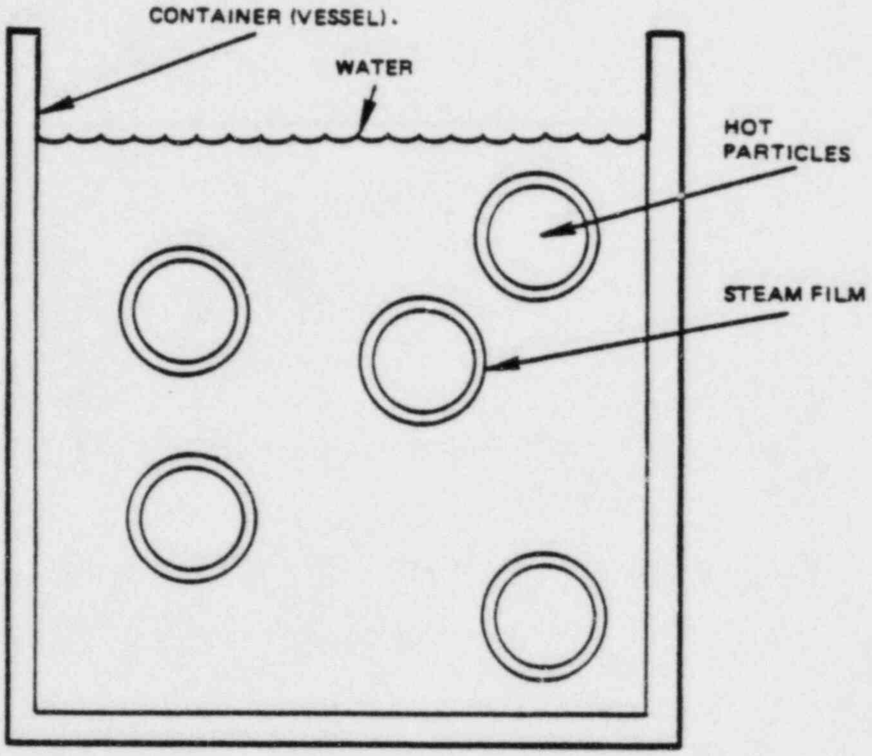

Figure H.5-9. Fragmentation in a Film Boiling Mode

GESSAR-II Appendix C Event Trees (156 pages)

AND

GESSAR-II Appendix D Fault Trees (309 pages)

C.1.3.4 Symbols Used in Containment Event Trees (Continued)

E_O is the probabilility that following a loss of primary containment integrity and/or suppression pool saturation, no RPV makeup water is injected from sources external to the containment, such as the condensate storage tank (CST) because of equipment failure or human errors.

E_T is the probability that following a Class IV ATWS event, the operator will not temporarily reduce the RPV continuous blowdown into the containment by throttling the RPV makeup and lowering the RPV water level below the top of the active fuel.

W_N is the probability that following a Class IV ATWS event and a RPV blowdown to the containment, adequate containment heat removal is not maintained, because of equipment failure or human errors.

C.1.4 Event Tree Example

For illustration purposes, an example event tree for the reactor shutdown initiating event is given in Figure C.1-2. The initiating event is given as the first branch in the far left column of the event tree. The initiating event name, symbol, and frequency of occurrence (events/year), are provided at the top of the column.

The tree is developed further by identifying the system functions required for successful termination of the event. These are presented in the approximate chronological order of occurrence. The success and failure states of each system function are given as

C.1.4 Event Tree Example (Continued)

branches in the tree. The upper branch represents success and the lower branch represents failure. If a prior system function directly leads to a success or failure during the accident sequence, analysis of the remaining system functions is not necessary. The information given at the top of the column for each system function is the name of the system success and the symbol for conditional failure probability. The value for the system failure probability is shown on the lower branch.

The accident sequences (event tree branches) terminate at the far right column. The sequence symbol, classification of effect, and frequency of occurrence is given for each tree branch. The classification of a sequence results either in successful termination (designated by "OK"), a core damage or loss of containment heat removal (designated by the containment event tree name, such as, CT2T, where the sequence is developed further) or a sequence which is developed further in another accident event tree (e.g., the sequence, T_MF_O, representing unplanned reactor shutdown is included in the turbine trip event tree). The frequency of each branch is given by the product of the initiating event frequency and conditional probabilities of the system functions in the accident sequence.

#3

APPENDIX D: FAULT TREES

The accident event trees in Appendix C are used to identify the key system functions that are involved in each accident sequence. Appendix D presents the Boolean models of combinations of components, systems or functions used to provide probabilistic values for the accident event trees. Boolean combination is necessary in those instances where there are common dependencies among systems or functions. Examples of such dependencies are electric power, instrument air, common sensors, service water and the requirement that maintenance on one safety system be carried out exclusive of maintenance on certain other safety systems.

The containment event trees in Appendix C are used to model the response of the containment to the accident sequences. The initiating events for the containment event trees are the output sequences from the accident event trees. The branches or nodes in the containment event trees represent the response of the containment to the characteristics of the accident sequences.

In Appendix C, each branch point (or node) in the event trees has a conditional probability of occurrence and a complementary probability of not occurring. Appendix D provides the derivation of the event tree probabilities, usually from (or involving) the basic failure rate data in Appendix A. Thus, to derive the value on the event trees, basic failure rate data for components, logic and human action are applied to the fault tree models, incorporating appropriate operating time and test intervals to obtain key system or function availabilities. The system or function availability is then tailored to the individual accident sequence event trees, taking into account interdependencies and the specific conditions of each event.

This appendix is organized in two sections. Section D.1 contains functional fault trees which model the interaction of several systems to provide inputs to the event trees. Section D.2 provides system level fault trees for the 14 systems that were modelled and analyzed. The fault trees utilize symbols consistent with the current state-of-the-art (Reference D.1-1 in Section D.1.1).

D.1 DERIVATION OF EVENT TREE PROBABILITIES

This section provides derivation of the input probabilities for the branches of the accident event trees and containment event trees in Appendix C. Section D.1 is organized as follows:

D.1.1 Scram and ATWS

D.1.2 Reactor Pressure Control

D.1.3 High Pressure Coolant Injection

D.1.4 Low Pressure Coolant Injection

D.1.5 Containment Heat Removal

D.1.6 Offsite Power

D.1.7 Containment Event Tree Quantification

D.1.1 Scram and ATWS

Table D.1.1-1 provides the event tree failure probabilities for scram and ATWS events. The following paragraphs provide the basis for values given in Table D.1.1-1.

D.1.1.1 Failure of Scram and ARI

Fast reactivity shutdown is accomplished by the scram system. A detailed analyses of the BWR scram system reliability was completed in 1976 (NEDE-21514) and the unavailability was estimated to be 5 x 10^{-6}/year (including common cause failure). The scram